N64 14286
CODE-1
CR-55307

50 p.

UNPUBLISHED PRELIMINARY DATA

TRANSOR DECISION FUNCTIONS AND STATISTICAL MEASUREMENT OF QUALITY

Contract Nasw-572
Reference WGD-38521

September 1963

OTS PRICE

XEROX $ 4.60 ph.

MICROFILM $ 1.70 mf.

Westinghouse Electric Corporation
Electronics Division
P. O. Box 1897 Baltimore 3, Md.

Special Technical Report No. 4

~~On~~

Transor Decision Functions

And

Statistical Measurement of Quality

(NASA Contract Nasw-572)

Reference WGD-38521

(NASA CR-55307)

OTS: $4.60, $1.75 mf

by

R. S. Bray,
P. A. Jensen, and
C. G. Masters

September 1963 50 p ref

9431008

~~The~~ Westinghouse Electric Corporation
Electronics Division
~~Box 1897~~, Baltimore 4, Maryland

APPROVED:

~~S. E. Lemak~~, Director
Advanced Development Engrg.

38521-5050

ABSTRACT

14286

The following report is in two parts. Part One describes the progress which has been made in evaluating a new type dynamic decision function. Part Two briefly describes several methods which have been considered for estimating the probability of mission success for redundant systems which may contain internal failures. The parts are completely separate except for the common bibliography found at the end. The remaining paragraphs of this abstract indicate the content of the individual parts.

Part One

This portion of the report describes the Transor class decision function as it might be used in a multiple-line restoring circuit application. Mathematical reliability models are derived which describe the Transor operation in different failure environments.

Part Two

This part of the report contains procedures which are being developed to aid in the determination of the ability of a redundant system to perform a mission of stated duration. It is proposed that the system be tested at the beginning of the mission to gain information on:

1. the number and location of failed circuits in the system
2. the failure rates of the system's circuits.

Several techniques are presented which show how to use this data to estimate the mission reliability. This estimate will be a basis for determining the acceptability of the system. One technique is presented which judges the acceptability of the system without a reliability estimate.

AUTHOR

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF ILLUSTRATIONS

PART ONE

I. INTRODUCTION

In recent years many novel schemes have been proposed to improve digital system reliability through the use of "redundant" equipment. Several of these, patterned after a concept of Von Neumann,[1] require a "restoring organ," "restorer" or "voter" to be placed after each set of redundant signal processors which perform a particular subsystem function. A restoring organ receives an input from each member of the associated set of processors. From these nominally identical input signals, the restoring organ produces an estimate of the correct subsystem output based on one or more specified decision criteria. It should be noted that the restorer does not perform any data processor function but acts as an error correcting transmission channel connecting two signal processors.

It has been shown in the literature[2] that the theoretically most efficient restoring organ is one that is capable of adapting itself to changes in the reliability of inputs. Specifically, for threshold type organs it has been shown that the optimum use of n unreliable versions of the same signal could be achieved by dynamically weighting each input in accordance with its relative reliability. Inputs which have a past history of being more reliable are given the heavier vote weights, and the unreliable inputs the lighter vote weights. The ideal restoring organ would sense the unreliable inputs and decide on the optimal vote weights. By efficiently tailoring the restoring organ to its ever-changing environment, significant improvement could be achieved over the presently popular majority restoring circuits.

In studying adaptive restoring organs, Westinghouse has shown[3] that circuit implementation of adaptive restoring organs for the specific requirements of redundant spaceborne systems is not yet practical. The complex circuitry required under the present "state of the art" to perform the adaptive function results in machines too cumbersome and unreliable to compete with less sophisticated redundant systems. This does not mean though that the present restoring organs used in redundancy techniques are adequate and cannot be improved upon.

The purpose of this study is to investigate a new restoring organ proposed by Westinghouse, called the Transor[4]. A characteristic of many failed subsystems is their tendency to have steady-state outputs as their dominant failure mode. In Transor, steady-state outputs are automatically deweighted by detecting only changes in states rather than the absolute states themselves. In an environment where the probability of steady state

---

[1, 2, 3, 4] See Bibliography

failure is relatively high, a restoring organ which ignores its steady-state inputs can derive a correct output with less than a majority of working inputs.

The salient characteristics of the Transor restoring organ are best shown by contrasting them to the corresponding characteristics of a majority restoring organ. The majority organ was chosen as a reference base because of its similarity in function to the Transor and because it is presently the most widely used restoring organ.

II. RESTORING CIRCUIT MODELS

A. THE TRANSOR DECISION FUNCTION

To be consistent with the terminology adopted by the other investigators of the Westinghouse Electronics Division, the term "restoring circuit" will be used to denote one functional unit of a restoring organ or restorer. A very general block diagram of a Transor restoring circuit having binary inputs $(x_1, x_2, \ldots x_R)$ and an output z is shown in figure T-1.

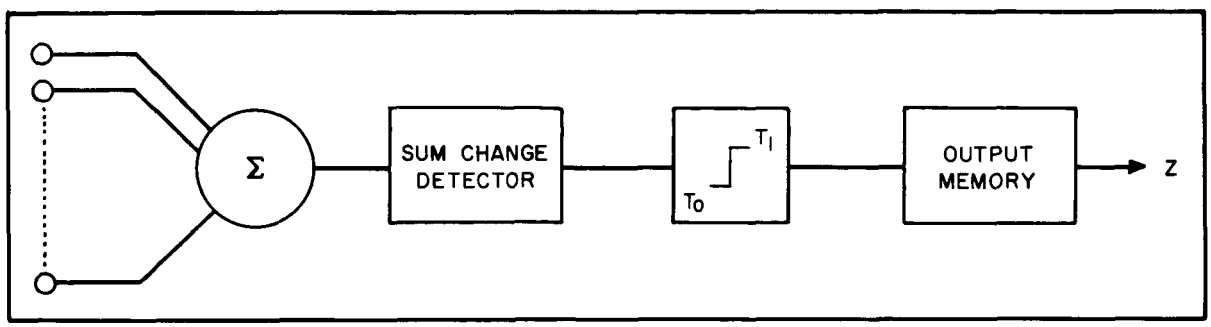

Figure T-1. Transor Restoring Circuit

Some of the salient characteristics of a Transor Restoring circuit are noted below:

1) It has memory

2) It operates only on the number of changes in the states of individual inputs between two adjacent bit times, (t - 1) and (t).

3) It is a binary voting element with a binary output.

4) It has two thresholds, not necessarily of the same magnitude, which combine with the states of the input at (t - 1) and (t) to determine the element output.

The functional relationship, describing the Transor Decision function can be stated as follows

$$Z^{(t)} = f\left[Z^{(t-1)}; (x_1, x_2 \text{--} x_R)^{(t)}; (x_1, x_2 \text{--} x_R)^{(t-1)}; T_o; T_1\right] \quad (1)$$

The number of binary Ones appearing on its inputs during each bit time are summed and compared with the number present during the previous time period. If the change is positive and greater than a given threshold T_1 then the output z is forced to a binary One. If the change is negative and greater in magnitude then a second threshold, T_o, the output is forced to a binary Zero. If neither threshold is exceeded, the output does not change from its previous state. This operation may be summarized by the following decision rule statements.

$$\sum_{o}^{R} x_i^{(t)} - \sum_{o}^{R} x_i^{(t-1)} \geq T_1 \rightarrow Z^{(t)} = 1 \tag{2}$$

$$\sum_{o}^{R} x_i^{(t)} - \sum_{o}^{R} x_i^{(t-1)} \leq -T_o \rightarrow Z^{(t)} = 0 \tag{3}$$

$$-T_o < \sum_{o}^{R} x_i^{(t)} - \sum_{o}^{R} x_i^{(t-1)} < T_1 \rightarrow Z^{(t)} = Z^{(t-1)} \tag{4}$$

B. THE THRESHOLD DECISION FUNCTION

The threshold model* consists of a black box having a certain number of binary inputs $(x_1, x_2 \ldots x_R)$ and an output z. At any bit time (t) the state of the output line z is a function of the state of the input lines and the threshold T. A general relationship similar to equation (1), but describing the threshold decision function may be delineated by the following expression.

$$Z^{(t)} = f \left[(x_1, x_2, \ldots x_R)^{(t)} ; T \right] \tag{5}$$

If the output, z, can assume either a Zero or One state, the threshold restoring circuit makes a decision to force its output to the One state under the following decision rule:

---

* The majority gate is a threshold model with $T = \frac{R+1}{2}$, where R is the number of inputs.

If

$$\sum_{o}^{R} x_i^{(t)} \geq T \rightarrow Z^{(t)} = 1 \tag{6}$$

and to the Zero state when

$$\sum_{o}^{R} x_i^{(t)} < T \rightarrow Z^{(t)} = 0 \tag{7}$$

III. FAILURE MODES

A. TRANSOR RESTORING CIRCUIT VULNERABILITY

Before the reliability of any Transor network can be expressed in a meaningful mathematical form, the failure modes of the individual subsystems appearing at the Transor's inputs must be explicitly stated.

A characteristic of Transor is its ability to differentiate between transistional and steady-state failures. This property creates failure modes different from those of threshold decision. Specifically, a signal processor is assumed either to be working correctly or failed into one of the following modes:

1. The transitional mode, in which extra Ones and/or extra Zeros appear at the output, and
2. The steady-state mode, in which the output permanently remains in a single state.

A transition (figure T-2) is defined as the rise or fall of a pulse during its switching time. The restoring circuit executes a decision by vector summing the change

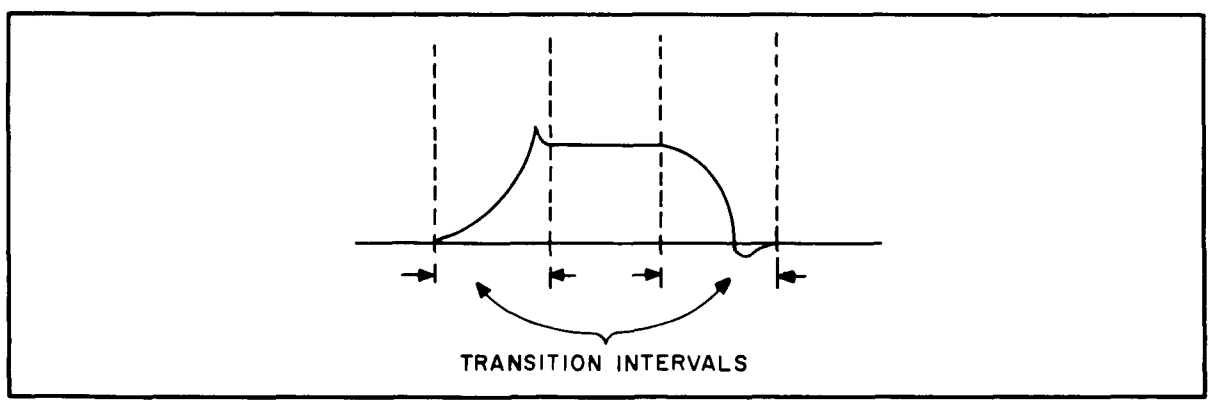

Figure T-2. Transition Intervals

in input pulses on the R redundant lines during the vote interval and a decision is made according to the decision rules (2) through (4). The term "extra One" implies a one has appeared on a signal processor's output when it should have been a Zero. By going to the wrong state a signal processor creates a wrong transition which is voted by the Transor. Wrong transitions can occur through diode failures in the gating section of diode-transistor

type signal processors. These failures sporadically generate "extra" Ones or "extra" Zeros as a function of the information at the gate's inputs. To illustrate, consider a three input Transor voting on the output of a network of redundant AND gates. The state of the binary inputs may be represented by the state vector $S_i^{(t)}$ below.

$$S_i^{(t)} = \begin{bmatrix} x_1^{(t)} \\ x_2^{(t)} \\ x_3^{(t)} \end{bmatrix}$$

In figure T-3 a diode is assumed to have opened in branch (1) of two of the gates causing those branches to appear as Ones. An erroneous One will appear at the gate's output whenever a correct Zero appears on those inputs and correct Ones appear on the remainder of the inputs. However, if all the input diodes open or an output element fails, the gating function will be destroyed, and the output will assume a steady-state. A method for determining the probability that a signal processor will fail into either of these two modes is discussed in Appendix I.

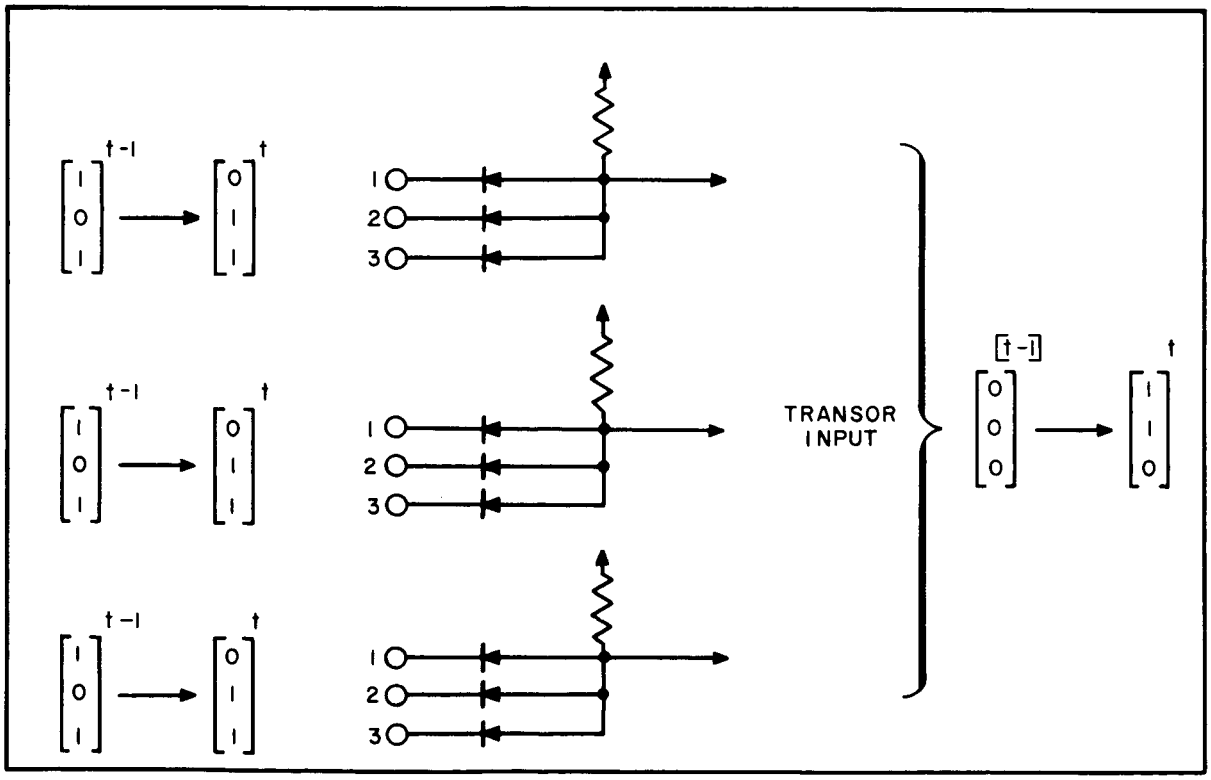

Figure T-3. Generation of Wrong Transitions in Redundant AND Gates

Because transitions are vector quantities their occurrence in the wrong direction may threaten Transor performance in three ways:

1. Wrong transitions cancelling correct transitions.
2. Wrong transitions occurring while the correct inputs remain in the same state (a series of Ones or Zeros). During this time the correct inputs have lost their voting power.
3. Wrong transistions temporarily simulating steady-state failures.

Wrong transitions produced by "extra Ones" and/or "extra Zeros" over a sequence of bit times can result in "error correlation" and create a variety of failure modes, subject to the nominally correct input states to the Transor for the considered sequence.

Figure T-4 shows this more clearly when state vectors are used to represent the inputs to a five input Transor. Inputs x_1 and x_2 are assumed to have failed and capable of randomly producing wrong transitions in either direction, i.e, extra Ones or Zeros. No inputs are assumed failed to a steady-state. For definiteness all inputs at time (t) may be assumed correct. In the following bit times (proceeding to the right) several failure patterns are possible for each nominally correct input state. At (t+1) the states (2), (3), (4), and (5) are considered among the possible states (four other possible states including (1) have been omitted as repetitious). Observe that sequence (1) → (2) is the most damaging because only the wrong transitions have any voting power. For a threshold set as low as two this would result in a wrong decision. The sequence (1) → (5) represents a possibility in which both erroneous inputs have temporarily "stuck" in one state simulating a temporary steady-state. The sequences (1) → (3) and (1) → (4) are the most likely possibilities in which one of the failed inputs is temporarily correct. In the next bit time (t + 2) transitions to the possible states (3), (4), (5) and (6) and (7) are considered (again repetitions are omitted). Shown here are the cancellation effects caused by the introduction of errors on the previous bit time, demonstrating the "error correlation" inherent in Transor. The sequence (2) → (5) is the most damaging because any threshold greater than one would have resulted in a wrong decision. Observe the tradeoff conflict created by the necessity for setting the threshold at a value greater than two in the sequence (1) → (2) and the same threshold at a value less than two in the sequence (2) → (5) in the following bit time. Clearly there must exist an optimum threshold. Inclusion in figure (4) of transitions from states (4) and (5) would have produced no new failure modes since they are but the duals of (2) and (3).

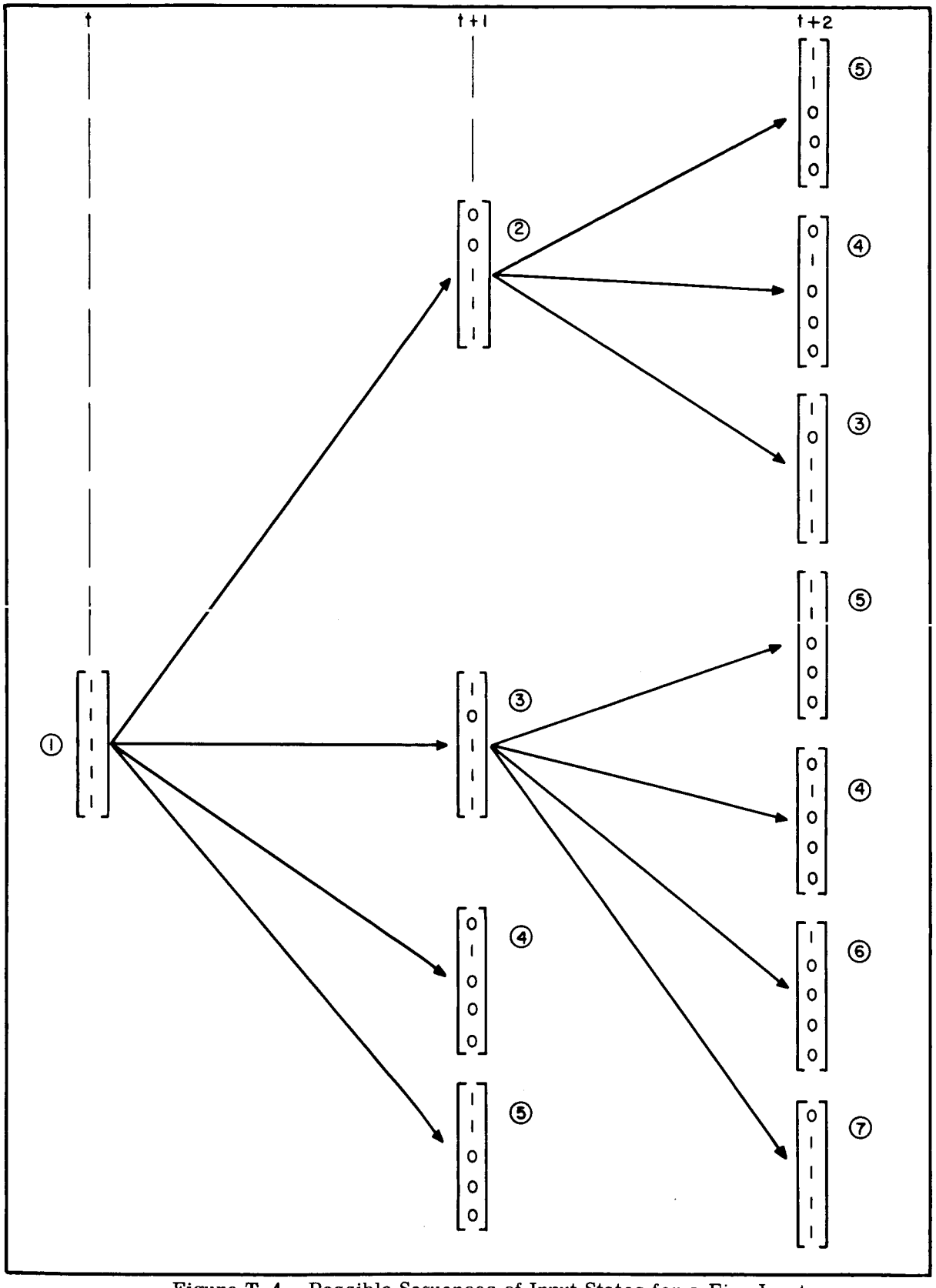

Figure T-4. Possible Sequences of Input States for a Five Input Transor Over Two Bit Times

B. THRESHOLD RESTORING CIRCUIT VULNERABILITY

A threshold restoring circuit makes a decision at time (t) by summing the number of binary Ones appearing momentarily at its inputs. The decision is independent of the input state at time (t - 1). By virtue of decision rule (6) if the number of errors appearing on the restorer's inputs is greater than the threshold T the restorer makes the wrong output decision. As opposed to Transor, the threshold device cannot differentiate between pure wrong transitions and steady-state failures so that both failure modes may be lumped together. To illustrate, consider a three-input threshold restoring circuit whose threshold is set at two (T = 2). For definiteness assume that x_1 and x_2 at time (t) are in error and in the same state and x_3 is correct as indicated below.

$$\begin{bmatrix} x_1^{(t)} \\ x_2^{(t)} \\ x_3^{(t)} \end{bmatrix} = \begin{bmatrix} \bar{x} \\ \bar{x} \\ x \end{bmatrix} \rightarrow Z^{(t)} = \bar{x}$$

Under this condition a wrong decision will be made. This may be considered a "worst case" failure mode because the alternate situation is possible where x_1 and x_2 have failed into opposite steady states.

$$\begin{bmatrix} 1 \\ 0 \\ X_3 \end{bmatrix} \rightarrow Z = X_3$$

In this case the errors nullify each other and the restoring circuit's output will follow the single correct input (x_3). In most reliability analyses the "worst case" is assumed, and any two failures in a set of restoring circuit inputs are assumed to cause system failure.

IV - RELIABILITY ANALYSIS

A. RELIABILITY DEFINED

In keeping with the usual concept of reliability, the reliability of a Transor restoring circuit will be defined as the probability that it never makes a wrong decision during its mission time. For analysis purposes the transor itself is assumed perfectly reliable, i.e., a wrong decision is never made through component failure within the Transor itself. In part III it was shown that errors appearing on the Transor inputs in a particular bit time could be correlated with errors that appeared on adjacent bit times to produce unique failure modes. Two of these were:

(1) Cancellation effects

(2) Simulated steady-state

In the following discussion it will be shown how these failure modes may be "built in" to reliability models by using multinomial expansions. Analytical models formulated in this manner may be easily compared with models for threshold reliability.

B. OUTPUT MODES DEFINED

Any output of a binary signal processor can be classified into one of six mutually exclusive classes over the element's mission time. These are:

1) Correct

2) Continuous Zero state

3) Continuous One state

4) Extra Ones but no extra Zeros

5) Extra Zeros but no extra Ones

6) Both extra Ones and Zeros.

Moreover the output of a system, composed of binary signal processors may be defined by the six mutually exclusive classes above. Each of these classes will be assigned the following probability measures in conformance with the Transor decision rules.

1) p; the probability that the output is correct

2&3) q_s; the probability that the output is either a continuous Zero or a continuous One.

4) q_1; the probability that the output generates extra Ones, but not extra Zeros.

5) q_o; the probability that the output generates extra Zeros, but not extra Ones

6) q_{10}; the probability that the output generates both extra Ones and Zeros randomly.

Note that the measure q_s is the result of the union of classes (2) and (3). The transitional probabilities q_1, q_o and q_{10} are defined to represent only the probabilities that a particular set of components, whose failure will cause wrong transitions to be generated randomly, will fail.

C. UPPER BOUND ON TRANSOR RELIABILITY

An upper bound on reliability is easily obtained by excluding all but steady-state failures from the environment. If β is a random variable denoting the number of correct transitions (or working inputs) and γ the number of inputs failed to a steady-state; a probability density function may be defined over the sample space as

$$\emptyset = \binom{R}{\beta, \gamma} P^{\beta} q_s^{\gamma}$$

Since Transor ignores steady-state failures the only criterion for a correct decision is that

$$\beta \geq T_o$$

$$\beta \geq T_1$$

The corresponding limits on γ are

$$\gamma \leq R - T \tag{8}$$

where $T_o = T_1 = T$. The reliability is

$$R_{U.B.} = \sum_{\beta = T}^{R} \binom{R}{\beta} P^{\beta}(1 - P)^{R - \beta} \tag{9}$$

In an environment capable of producing only steady-state failures, the maximum reliability and error correction capability is obtained by setting T = 1. This is the optimum threshold. From equation (8) we see that Transor can correct at best R - 1 failures in an order R redundant system.

D. TRANSOR RELIABILITY FOR STRICTLY ASYMMETRIC FAILURE MODES

Excluding from the mutually exclusive ways an environment can fail class (6) and either class (4) or (5) limits transitional failure modes to states (2), (3), (4) and (5) in fig. (4). Of these the sequence (1) → (2) is the "worst case". For definiteness let it be assumed that Transor inputs may produce only extra Zeros and steady-state failures. Let α_o be a random variable denoting the number of wrong transitions to the Zero state.

The density function on this sample space is

$$\emptyset = \binom{R}{\beta, \gamma, \alpha_o} P^{\beta} q_s^{\gamma} q_o^{\alpha_o}$$

A wrong decision will be made unless

$$\alpha_o \leq T_o - 1$$

Since it is necessary that

$$\beta \geq T_o$$

the limits on γ must be

$$\gamma \leq R - T_o - \alpha_o$$

The reliability is

$$R = \sum_{\alpha_o = 0}^{T_o - 1} \sum_{\gamma = 0}^{R - T_o - \alpha_o} \binom{R}{R - \alpha_o - \gamma, \gamma, \alpha_o} P^{R - \alpha_o - \gamma} q_s^{\gamma} q_o^{\alpha_o} \qquad (10)$$

E. TRANSOR RELIABILITY FOR MUTUALLY EXCLUSIVE OUTPUT FAILURE MODES

The scope of the environment considered in part D can be broadened to include both the mutually exclusive classes (4) and (5). Each input may be failed to either steady-state, extra Ones or extra Zeros (but not both). The failure modes (figure T-5) may be represented in a manner similar to figure T-4; inputs x_1 and x_2 assumed failed in one of the four mutually exclusive ways listed above.

The sample space may be described by the density function

$$\emptyset = \binom{R}{\beta, \alpha_o, \alpha_1, \gamma} P^{\beta} q_o^{\alpha_o} q_1^{\alpha_1} q_s^{\gamma}$$

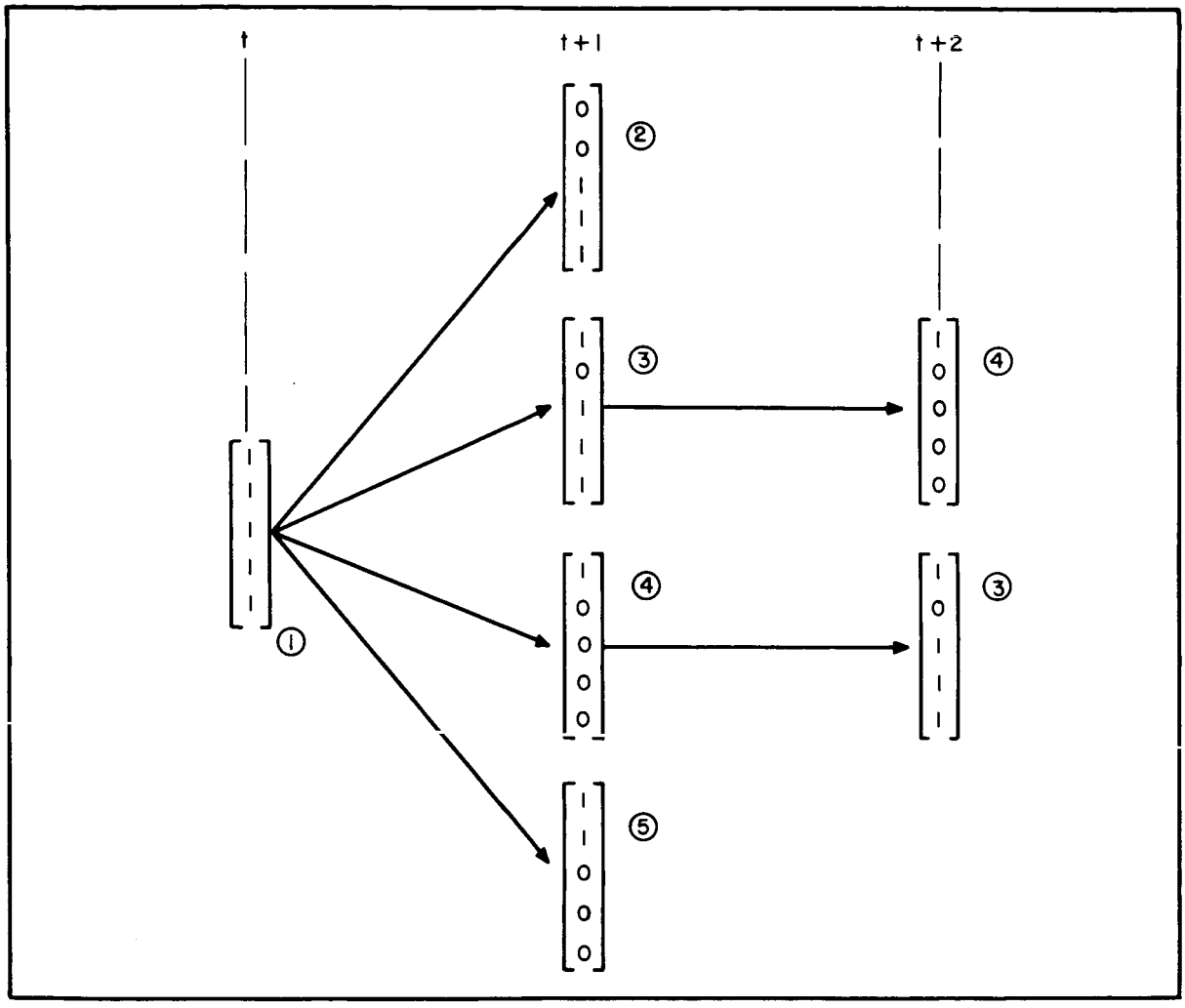

Figure T-5. Possible Sequences for a Five-Input Transor with Mutually Exclusive Output Failure Modes

The sequence (1) → (2) in figure (5) implies that a Transor will make a wrong decision unless

$$\alpha_o \leq T_o - 1 \tag{11}$$

and its dual

$$\alpha_1 \leq T_1 - 1. \tag{12}$$

From the sequences (1) → (3) and (1) → (4) respectively

$$\beta + \alpha_1 \geq T_1 \tag{13}$$

$$\beta + \alpha_o \geq T_o \tag{14}$$

for a correct decision. However examination of the sequences (3) → (4) and (4) → (3) show that inequalities (13) and (14) do not represent "worst cases". "Error correlation" between the bit times (t + 1) and (t + 2) have produced a temporary steady-state. A correct decision will be made only if

$$\beta \geq T_o \tag{15}$$

$$\beta \geq T_1 \tag{16}$$

From (15) and (16)

$$\gamma \leq (R - T_o) - \alpha_1 - \alpha_o \tag{17}$$

$$\gamma \leq (R - T_1) - \alpha_1 - \alpha_o \tag{18}$$

Of these last two inequalities the number of allowable steady-state failures, γ, will be governed by the highest threshold, T_o or T_1.

The reliability will take the form

$$R = \sum_{\alpha_0=0}^{T_o-1} \sum_{\alpha_1=0}^{T_1-1} \sum_{\gamma=0}^{R-T_o-\alpha_o-\alpha_1} \binom{R}{R-\alpha_o-\alpha_1-\alpha,\ \alpha_o,\ \alpha_1,\gamma} p^{R-\alpha_o-\alpha_1-\gamma} q_o^{\alpha_o} q_1^{\alpha_1} q_s^{\gamma} \tag{19}$$

where T_o is assumed $> T_1$.

F. TRANSOR RELIABILITY FOR A SYMMETRICAL ENVIRONMENT

A symmetrical environment utilizing Transor decision will be defined as the mutually exclusive classes (1), (2), (3) and (6). Wrong transitions may occur in both directions and at random. Therefore $\alpha_o = \alpha_1 = \alpha$ and $T_o = T_1 = T$. The density function on this sample may be written as

$$\phi = \binom{R}{\beta,\ \alpha,\ \gamma} p^{\beta} q_{10}^{\alpha} q_s^{\gamma}$$

From figure T-4 it can be seen that a wrong decision will be made unless

$$\alpha \leq T - 1 \tag{20}$$

and

$$\beta - \alpha \geq T \tag{21}$$

From (21)

$$\gamma \leq R - T - 2\alpha \tag{22}$$

Therefore the reliability for the symmetrical environment is

$$R = \sum_{\alpha=0}^{T-1} \sum_{\gamma=0}^{R-T-2\alpha} \binom{R}{R-\alpha-\gamma, \alpha, \gamma} p^{R-\alpha-\gamma} q_{10}^{\alpha} q_s^{\gamma} \tag{23}$$

V. CONCLUSION

The dynamic characteristics of the Transor decision function make this type restoring circuit unique to the present art. The mission of this part of the Failure Free Systems Study has been to evaluate the potential usefulness of the Transor as a restoring circuit.

Primarily because it is most commonly used in present redundant equipment, the threshold type restoring circuit has been chosen as the reference point for the evaluation primarily. It has been hypothesized that, if it can be shown that the Transor failure masking capability compares favorably to that of the threshold restoring circuit, further development, including the construction of a breadboard model, should be justified.

The results of section IV have shown that there are certain environments in which Transor can be used to advantage in improving system reliability. For example, the maximum error restoring capability of Transor is shown to be R-1 failures of R redundant lines in an environment free from transitional failures. This is a significant improvement over the majority threshold restoring capability under the same conditions. There is need for caution, however, for in environments where symmetrical transitional errors are possible error correlation may make Transor performance inferior to threshold. From the reliability models, a tradeoff may be determined in terms of the output error probabilities of the environment.

The work done up to this point represents only a first step in Transor decision study. Work yet to be done includes: (1) a general Transor reliability model incorporating all the possible failure modes and (2) a decision rule for determining an optimum threshold.

In addition to continuing the analytical effort described in this report, a computer simulation program is being written to aid in the task (1) effort. This will be a relatively simple but versatile program designed to accommodate any set of restricting assumptions including those made in the four models derived in this report. The results of this report have shown a solution to task (2) would be desirable because of the tradeoffs between different failure modes. If the error probabilities of the signal processor outputs are known in the design stage maximum reliability can be bought for zero additional cost by a judicious choice of the thresholds.

VI. APPENDIX

Determination of the Reliability Parameters p, q_s, q_o, q_1, q_{10} in a Signal Processor.

In section IV it was shown that reliability models could be formulated in terms of the output error probabilities of a set of redundant signal processors. This section describes a method for determining these probabilities.

Consider a set X* which has for its members the n components of a signal processor. Each member (component) has two possible states:

x_i; the $i^{\underline{th}}$ member is working.

$\bar{x}_i$; the $i^{\underline{th}}$ member has failed.

Let each component have a reliability

$$P(x_i) = e^{-\lambda_i t}$$

and a probability of failure

$$P(\bar{x}_i) = 1 - e^{-\lambda_i t}$$

The probability measure on the sample space of X may be partitioned into the canonical form

$$\begin{aligned} 1 = {} & P(x_1 \cap x_2 \cap -- x_n) + P(\bar{x}_1 \cap x_2 \cap -- x_n) \\ & + P(x_1 \cap \bar{x}_2 \cap x_3 - - x_n) + \cdots + \\ & + P(\bar{x}_1 \cap \bar{x}_2 \cap - - \bar{x}_n) \end{aligned} \tag{24}$$

Briefly, the method requires determining the correspondence between groups of the terms in (24) and the individual terms in

$$1 = p + q_s + q_o + q_1 + q_{10} \tag{25}$$

Obviously the parameter p, that the signal processor output is correct is

$$p = P(x_i \cap x_2 \cap \ldots . x_n)$$

The remaining 2^n-1 terms in (24) are mapped into the four remaining parameters in (25) by paritioning the set X into subsets whose members are defined by those components whose

* Summary of all the notation to be used is included on the last page of this appendix.

failure will result in one of the four mutually exclusive events described in part IV. Specifically let

X_{ss} be the set whose failure results in either a steady-state Zero or One.

X_1 be the set whose failure results in extra Ones.

X_o be the set whose failure results in extra Zeros.

X_{10} be the set whose failure results in extra Ones and Zeros.

Since each component may fail by shorting or opening, these two modes will determine membership in one or more of the above sets. If the probability of a component shorting given that its failed, $P(x_i^s \mid \bar{x}_i)$, is ρ_i then the joint probability of x_i failing and shorting is

$$P(\bar{x}_i \cap x_i^s) = P(x_i^s) = P_i(1 - e^{-\lambda it})$$

Let the probability of an x_i opening given that its failed the $P(x_i^o \mid \bar{x}_i)$

Then

$$P(x_i^s \mid \bar{x}_i) + P(x_i^o \mid \bar{x}_i) = 1$$

and

$$P(x_i^o \mid \bar{x}_i) = 1 - \rho_i$$

Also since for each x_i the events working, shorted or opened are mutually exclusive the probability of a component <u>not</u> shorting is

$$P(\bar{x}_i^s) = P(x_i \cup x_i^o) = 1 - \rho_i (1 - e^{-\lambda it})$$

To illustrate the technique a NAND gate will be analyzed using the test results contained in an earlier Westinghouse report.[5]

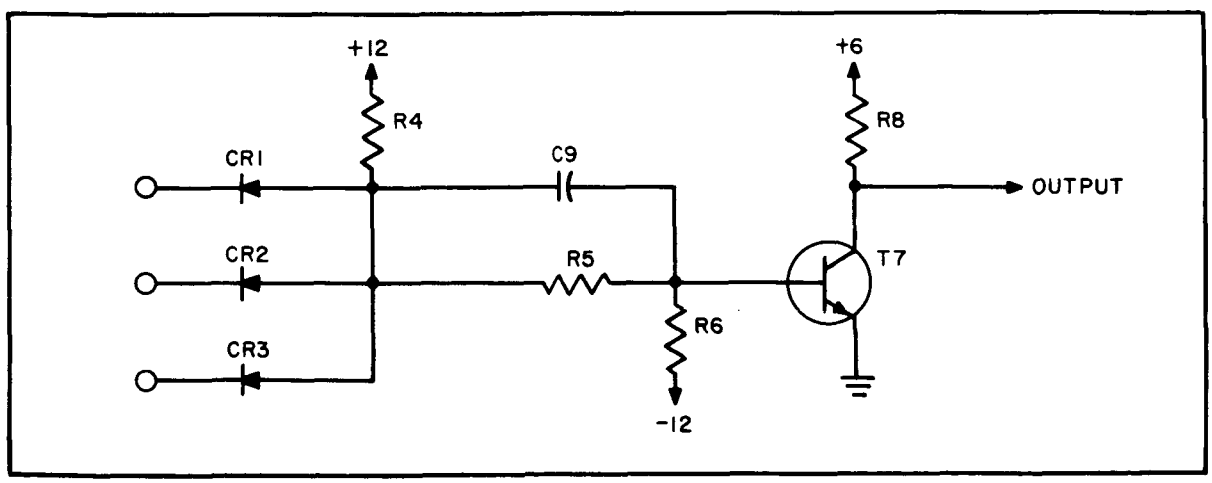

Figure AT-1. NAND GATE

The pertinent results are included below.

1. AND gate input diodes; CR1, CR2, CR3

A. OPEN - Any open circuit input is equivalent to a logical "one" on that input; it cannot inhibit the AND gate.

B. SHORT - A shorted diode will not affect the ability to perform the AND function if that input has low impedance to ground in the "zero" state and high impedance to a positive voltage in the "one" state. The line with a shorted diode is no longer isolated from other inputs; that line is shorted to the AND gate output and may, therefore, be an incorrect "zero".

2. AND gate resistor; R4

A. OPEN - The AND gate has no voltage available to drive current into the transistor base, so the NAND gate output remains a "one".

B. SHORT- This will cause a low impedance path from the +12 volt power supply through the input diodes to all of the inputs to the gate. If any of these inputs are from NAND gate transistors which are conducting, that input will also be a low impedance to ground. A low impedance path then exists from the power supply to ground, and a high current will flow through the diode and transistor according to the magnitude of the impedance of the power supply and components involved. In the tests observed, this current was not sufficient to damage the transistor or diode and did not blow the fuse on the power supply. However, if many inputs are from flip-flops, the clamp diode will turn on when the voltage exceeds the clamp voltage. A low impedance path then exists from the +12 volt power supply through the shorted AND gate resistor, the input diode, and may seriously overload the clamp voltage supply, depending how the clamp voltage is derived. In the tests observed, this current was sufficient to cause both the input diode and clamp diode to short and the clamp voltage to rise toward +12 volts.

3. Input resistor - capacitor; R5, C9

A. Resistor SHORT- The transistor base voltage will be the AND gate output. This will normally cause the transistor to conduct, so that the output will be "zero" for any logic input.

B. Resistor OPEN- This will cause the transistor to be off, so that the output will be a "one" for all logic inputs.

C. OPEN C9 - This does not adversely affect operation, unless the switching time is critical, in which case NAND gate turn-on time was increased from 65 nanoseconds with C9 to 80 nanoseconds without C9; turn-off time was increased from 25 to 45 nanoseconds in one approximate measurement with a constant load on the output of the circuit. The turn-on time was measured as the time from the input going positive above +1.6 v. until the output goes to +1.6 v. from the "one" state. The turn-off time was measured as the time from the input going negative below +2.4 v. until the output goes to +2.4 v. from the "zero" state.

4. Base bias resistor, R6

A. OPEN - This will normally cause the transistor to conduct, so that the output will be "zero" for any logic input, except that when the AND gate voltage is going negative from the "one" state, this voltage change is coupled across C9 and will turn the transistor off until the transient effect has ended.

B. SHORT- The short of the base resistor may cause damage to the output transistor, since -12 volts on the base exceeds the maximum rating of 5 volts for V_{EBO}. The output voltage will depend on the failure mode, if any, of the transistor. In three multiple failure tests that included short of the base bias resistor in a NAND gate, two transistors shorted base to collector, which resulted in a -12 volt output; one transistor shorted collector to emitter, which resulted in a "zero" output. The -12 volt output did not cause any significant difference than a normal "zero" output to the following circuitry.

5. Collector (output) resistor, R8.

A. OPEN- The removal of the output resistor does not affect the logical operation of the circuit, since any loads are also to positive voltage sources. The output rise time will be somewhat slower but the output will turn off faster because the output voltage in the "one" state is lower and the load current is less.

B. SHORT- The output voltage will be +6 volts; the current in the transistor will be high if the transistor is conducting. This current was not sufficient to cause permanant damage to the transistor in the observed tests.

6. Transistor, T7

The transistor may fail into any of several possible modes, but the circuit output will usually be a "one" unless a low impedance path exists from the output to ground, such as when the collector is shorted to emitter, or if the transistor is otherwise forced to remain conducting from collector to emitter.

From the test results the component failures may be categorized (below) into their effects on the NAND gate's output.

I Components Causing Failure into Steady State "1"

1) R4 Open
2) R5 Open
3) T7 (most modes result in a "1")

II Components Causing Failures into Steady State "0"

1) R5 short
2) R6 short
3) R6 open
4) CR1 and CR2 and CR3 open (together)

III Component Failures that will Produce Transitional Extra "Ones"

1) CR1 or CR2 or CR3 open
2) CR1 and CR2 open
3) CR1 and CR3 open
4) CR2 and CR3 open

From the three categories above may be formed the mutually exclusive sets

Set X_s	Probability of $X_s(i) = P\left[X_s(i)\right]$
$X_s(1)$: x_4^o	$(1-\rho_4)\left(1 - e^{-\lambda_4 t}\right)$
$X_s(2)$: $\bar{x}_5$	$1 - e^{-\lambda_5 t}$
$X_s(3)$: $\bar{x}_6$	$1 - e^{-\lambda_6 t}$
$X_s(4)$: $\bar{x}_7$	$1 - e^{-\lambda_7 t}$
$X_s(5)$: $x_1^o \cap x_2^o \cap x_3^o$	$\left[(1-\rho)(1 - e^{-\lambda t})\right]^3$

The probability of a steady-state failure is

$$q_s = \sum_{i=1}^{5} P\left[X_s(i)\right] - \sum_{i \neq j}^{5} P\left[X_s(i, j)\right] + \sum_{i \neq j \neq k}^{5} P\left[X_s(i, j, k)\right]$$

$$- \sum_{i \neq j \neq k \neq l}^{5} P\left[X_s(i, j, k, l)\right] + \prod_{i=1}^{5} P\left[X_s(i)\right]$$

Set X_o	Probability of X_o (i) = P $\left[X_o (i)\right]$
$X_o(1)$: $(x_1^o \oplus x_2^o \oplus x_3^o) \cap \bar{x}_4^o \cap x_5 \cap x_6 \cap x_7$	$3\,(1-e)\,(1-e^{-\lambda t})\cdot e^{-2\lambda t}\left[1-(1-\rho_4)\,(1-e^{-\lambda_4 t})\right]e^{-(\lambda_5+\lambda_6+\lambda_7)t}$
$X_o(2)$: $(x_1^o \cap x_2^o \oplus x_2^o \cap x_3^o \oplus x_1^o \cap x_3^o) \cap \bar{x}_4^o \cap x_5 \cap x_6 \cap x_7$	$3\left[(1-\rho)\,(1-e^{-\lambda t})\right]^2 e^{-\lambda t}\left[1-(1-\rho_4)\cdot(1-e^{-\lambda_4 t})\right]\cdot e^{-(\lambda_5+\lambda_6+\lambda_7)t}$

The probability of an extra zero is

$$q_o = \sum_{i=1}^{2} P\left[X_o\ (i)\right]$$

Observe from the set X_o that transitional errors will be caused by less than three of the input diodes failing through opening. In actuality the probability of a wrong transition for the member X_o (1) in the set X_o is the joint probability:

P (i $\frac{th}{}$ Diode open $\cap$ "O" on the i $\frac{th}{}$ input $\cap$

n-1 diodes working $\cap$ "1's" on the n-1 diodes $\cap$ no steady-state failures)

=P (i $\frac{th}{}$ Diode open). P (n-1 Diodes working). P ("O" on i $\frac{th}{}$ input $\cap$

1's on n-1 inputs $\Big|$ i $\frac{th}{}$ Diode open $\cap$ n-1 working). P (no steady-state failure)

The third term in the joint probability expression is the conditional probability expressing the fact that a wrong transition is a function of the information appearing at the gate inputs in any bit time. For all practical purposes this term may be set equal to unity due to the tremendous speed at which information is processed and the resulting short time between occurrance of all possible input states. This same reasoning may be applied to the other member X_o (2).

Note that a NAND gate possesses an asymmetric environment because there are no failure modes that can result in the exclusive classes X_1 or $X_{1\,o}$.

Thus the reliability of a Transor voting on the output of a network of redundant NAND gates can be defined by equation (10) in part IV.

The following notation was used in this appendix.

1) x_i, the event that the $i^{\underline{th}}$ component is working correctly.

2) $\bar{x}_i$; the event that the $i^{\underline{th}}$ component has failed.

3) $P(x_i)$; probability of the defined event (1)

4) $P(\bar{x}_i) = 1 - P(x_i)$

5) x^s ; the event that the $i^{\underline{th}}$ component has shorted

6) x^o ; the event that the $i^{\underline{th}}$ component has opened because the possibility space of each component is the logical union of

$$x_i \cup (\bar{x}_i \cap x^s) \cup (\bar{x} \cap x^o)$$

7) $P(x_i^s)$; the probability of (5)

8) $P(x_i^o)$; the probability of (6) = $1-P(x_i) - P(x_i^s)$

9) $\bar{x}^s$; the event that the $i^{\underline{th}}$ component has not shorted

10) $\bar{x}^o$; the event that the $i^{\underline{th}}$ component has not opened

11) $P(\bar{x}^s)$; the probability of (9)

12) $P(\bar{x}^o)$;the probability of (10)

13) $P(x^s \mid \bar{x}_i)$; the probability of the $i^{\underline{th}}$ component shorting given that its failed = ρ

14) $P(x^o \mid \bar{x}_i)$; the probability of the $i^{\underline{th}}$ component opening given that its failed. = $1-\rho$

PART TWO

I. INTRODUCTION

The problem of the pre-launch testing of spaceborne electronic systems is becoming more severe as the systems increase in complexity while decreasing in physical size. The testing problem will soon become much worse as systems are made redundant and in-flight tests are used to determine the successive actions of deep space probes. Tests can no longer be made adequately on the basis of a strict "working" or "failed" criterion because a redundant system may contain many internal failures and still be operating at the time of test. Such a system might easily have a much lower probability of successfully completing a mission than a functionally identical non-redundant system.

In addition, the large number of subsystems in a complex redundant network will make complete check-out (i. e. tests of each subsystem) virtually impossible. Consequently, a new method must be devised which will permit a statistical estimate to be made of the probability of mission success (reliability). This estimate must be based on the results of a limited amount of testing and should be as accurate as possible.

II. MISSION RELIABILITY

The problem may be stated more specifically as follows. A test of a redundant machine will be made at some time t_1. (It is expected that some failures will be found in the equipment, and the object of the test is merely to determine the number and pattern of the failures in the system.) From the test data, the probability that the redundant system under test will operate successfully throughout a mission which begins at time, t_1, and ends at time, t_2, given that the system is operating at t_1, is estimated. This probability is defined as the mission reliability (R) and is a function of the system organization, the state of the system at t_1, the failure rates of the parts of the system, the starting time (t_1) of the mission, and the mission's duration, $t_2 - t_1$. At some time t_0, which is less than t_1 or t_2, all circuits in the system are assumed perfect. As time progresses they are assumed to fail in a random manner with a constant failure rate. At t_1 when the system is ready to begin the mission, the system must be in one of a finite number of possible failure states. The failure states are determined by the number and location of failed circuits in the system. For example, consider the multiple-line redundant network of figure Q-1. A restoring circuit indicated by a circle will make a correct decision if at least two of its inputs are correct.

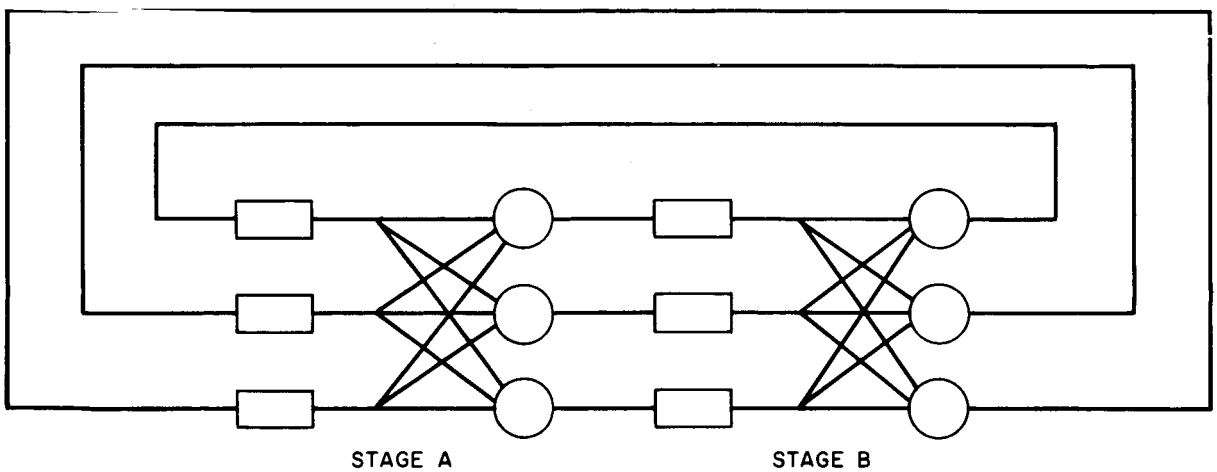

Figure Q-1. A Two Stage Example of a Redundant System

Assume for simplicity of explanation, that the restoring circuits of this system are perfectly reliable and that only signal processing circuits, indicated by rectangles, can fail. The possible failure states of this system are listed in colums 2 and 3 of Table I.

TABLE 1

1 Failure State	2 Number of Failures in Stage A	3 Number of Failures in Stage B	4 R_i * (t_2) **	5 P_i (t_1) ***
1	0	0	$\left[p_m^3 + 3\,p_m^2\,(1-p_m)\right]^2$	$\left[p^3\right]\left[p^3\right]$
2	0	1	$\left[p_m^3 + 3\,p_m^3\,(1-p_m)\right]\,p_m^2$	$\left[p^3\right]\left[3p^2\,(1-p)\right]$
3	0	2	0	$\left[p^3\right]\left[3\,p\,(1-p)^2\right]$
4	0	3	0	$\left[p^3\right]\left[(1-p)^3\right]$
5	1	0	$\left[p_m^3 + 3\,p_m^2\,(1-p_m)\right]\,p_m^2$	$\left[3p^2\,(1-p)\right]\left[p^3\right]$
6	1	1	p_m^4	$\left[3p^2\,(1-p)\right]\left[3p^2(1-p)\right]$
7	1	2	0	$\left[3p^2\,(1-p)\right]\left[3p^2\,(1-p)^2\right]$
8	1	3	0	$\left[3p^2\,(1-p)\right]\left[(1-p)^3\right]$
9	2	0	0	$\left[3p\,(1-p)^2\right]\left[p^3\right]$
10	2	1	0	$\left[3\,p\,(1-p)^2\right]\left[3\,p^2\,(1-p)\right]$
11	2	2	0	$\left[3\,p\,(1-p)^2\right]\left[3\,p\,(1-p)^2\right]$
12	2	3	0	$\left[3\,p\,(1-p)^2\right]\left[(1-p)^3\right]$

* $R\,(t_2)$ is the probability of correct system operation at time (t_2) given the 5^{th} failure state exists at t_1.

** All the p_m's in this column are probabilities that a circuit is successful at t_2, given it was successful at t_1.

*** All the p's in this column are probabilities that a circuit is successful at t_1, given it was successful at t_0.

TABLE 1 (Cont)

1 Failure State	2 Number of Failures in Stage A	3 Number of Failures in Stage B	4 R_i * (T_2) **	5 P_i (t_1) ***
13	3	0	0	$\left[(1-p)^3\right]\left[p^3\right]$
14	3	1	0	$\left[(1-p)^3\right]\left[3p^2(1-p)\right]$
15	3	2	0	$\left[(1-p)^3\right]\left[3p(1-p)^2\right]$
16	3	3	0	$\left[(1-p)^3\right]\left[(1-p)^3\right]$

* $R(t_2)$ is the probability of correct system operation at time (t_2) given the 5th failure state exists at t_1.

** All the p_m's in this column are the probability that a circuit is successful at t_2, given it was successful at t_1.

*** All the p's in this column are the probability that a circuit is successful at t_1, given it was successful at t_0.

For each of the failure states of Table 1, the reliability of the system can be calculated at t_2. This is done as follows: If the failure rate, λ , of a circuit is constant and known, the probability that a circuit is successful at t_2, given it is successful at t_1 is the expontential.

$$P_m = e^{-\lambda (t_2 - t_1)} \tag{1}$$

For the system to be successful at the end of the mission, two or three circuits in each stage must be successful. The probability that the system meets this requirement depends on the failure state of the system at t_1, and the value of p_m. For instance for failure states 3, 4, 7, 8 and 9-16, the probability of correct system operation must be zero because there are too many failures at t_1. Because R_i is defined as this probability, given the system is in the ith state at t_1:

$$R_i = 0 \quad \text{for } i = 3, 4, 7, 8, 9\text{-}16$$

For failure state 1, the reliability is the probability that two or three circuits are successful at t_2. Thus:

$$R_1 = \left[P_m^{\,3} + 3 P_m^{\,2} (1 - P_m)\right]^{\,2}$$

The reliability of the system for other failure states is shown in column 4 of Table 1.

Column 5 of Table 1lists the probabilities that the particular failure states will be present at t_1. The factor p in this column is the probability of success of a circuit at t_1 given the circuit was successful at t_0. These probabilities will find use in later discussions.

Two things must be known if the mission reliability of the system is to be determined with 100% confidence, the failure state of the system and the failure rates of the circuits (needed to calculate P_m). For large systems both these factors may be very difficult or impossible to determine exactly. To find the failure state of a system, the failure state of each stage must be known. This may require a considerable amount of testing, probably a test of all circuits in the system. The failure rates of the circuits can only be determined exactly with a test of an infinite number of circuits all operating under the same environments as the circuits in the system. Of course, with limited testing allowed at t_1 it is improbable that the exact failure state of the system can be found. Estimates and their accuracy are the subject of the remainder of this report.

III. PROCEDURES FOR ESTIMATING THE SYSTEM RELIABILITY

In the study of this problem, several ways have been proposed to estimate a system's mission reliability with varying degrees of accuracy and varying levels of confidence. Four of these are described below.

A. ESTIMATION OF THE EXPECTED VALUE OF MISSION RELIABILITY WITH ONLY THE INFORMATION THAT THE SYSTEM IS OPERATING AT t_1.

Using the design failure rates* one can estimate the mission reliability with only the information that the system is operating successfully at t_1. This is done using the equations representing the reliability of the system at time t given only that all circuits are operating successfully at time 0. The system reliability R (t) can be written as the probability of successful operation from time 0 to time t. The reliability of the system of figure 1 is:

$$R(t) = \left\{ p(t)^3 + 3 \left[p(t) \right]^2 \left[1 - p(t) \right] \right\}^2 \qquad (2)$$

$$\text{where } p(t) = e^{-\lambda t}$$

A plot of R(t) for the redundant system of figure Q-1 is shown in figure Q-2a.

---

* The design failure rates are those assigned to the circuits during the design of the system. They are generally derived from controlled life testing or components similar to those used in the circuits or from field tests of similar components.

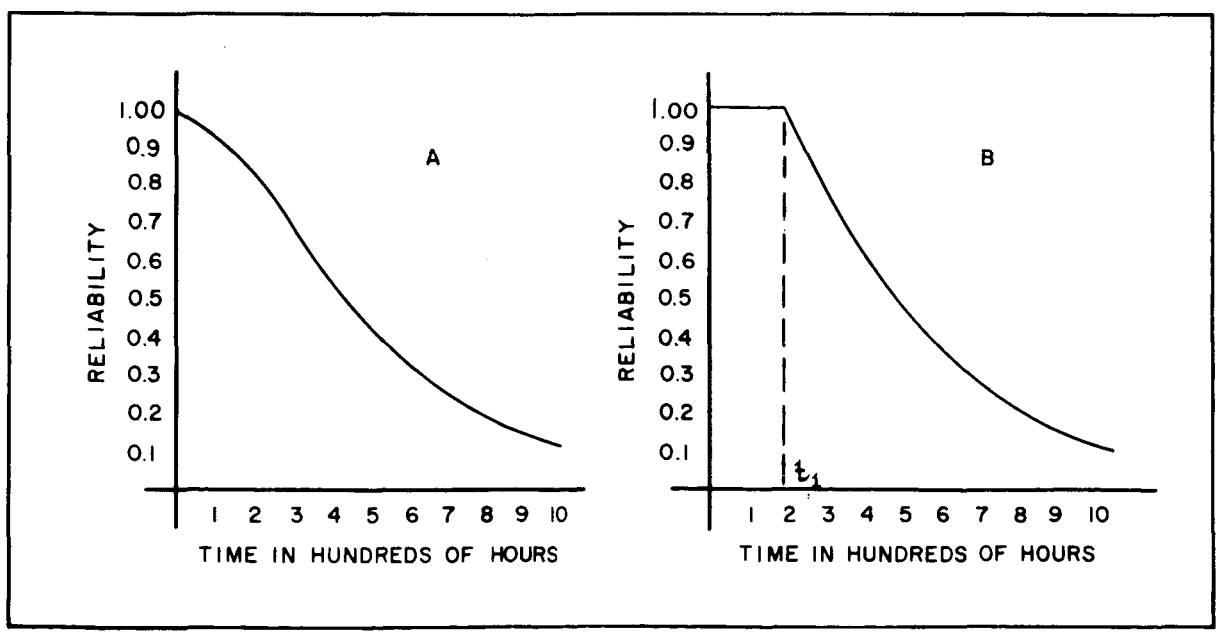

Figure Q-2. Reliability vs Time For a Redundant System.
A) With No Test at t_1.
B) With a Test Determining the Success of the System at t_1

If one tests the system at a time t_1 and finds it to be working successfully, this information can be used to adjust the system reliability for time greater than t_1 to take account of the condition of success at t_1. A curve must now be determined which gives the reliability of the system given successful operation at t_1. This is expressed as:

$$R\left[t \mid R(t_1)\right]$$

For $t \quad t_1$, the reliability must be unity, because it is assumed that once a system fails it stays failed.

Then:

$$R\left[t \mid R(t_1)\right] = 1 \qquad t < t_1 \tag{3}$$

For $t \quad t_1$, the reliability is:

$$R\left[t \mid R(t_1)\right] = \frac{R(t)}{R(t_1)} \qquad t > t_1 \tag{4}$$

This is derived from the definition of conditional probabilities.

$$P(A \mid B) = \frac{P(A \text{ and } B)}{P(B)}$$

A plot of equations (3) and (4) is shown in figure Q-2b for a particular t_1 and the system shown in figure Q-1.

Using equation (4) the mission reliability can be written:

$$R(t_2, t_1) = \frac{R(t_2)}{R(t_1)} \tag{5}$$

Thus, the mission reliability can be determined simply by using the reliability equations of the system and the design failure rates of the circuits of the system.

The question now arises, of what value is this result? First, assuming the failure rates used in the calculation of R are perfect, if a large number of systems were constructed and run until t_1, approximately $R(t_1) \times 100\%$ of them would be working. Throwing away all systems that were failed at t_1 and continuing the test until t_2, $R(t_2, t_1) \times 100\%$ of the population all systems working at t_1 will be working at t_2.

No information was given for this estimate about the failure state of the system at t_1, except that the system was in one of the failure states for which the system is successful. For the example, these are states 1, 2, 5 and 6. This limited information about the failure state makes it necessary to approximate the mission reliability by an expected value given that the system is in one of the four successful failure states. The approximation has a considerable effect on the accuracy of the estimate which is described in detail in Section IIIC of this report.

B. ESTIMATION OF THE EXPECTED VALUE OF MISSION RELIABILITY WITH TESTS AT t_1, HELPING TO ESTABLISH THE CIRCUIT FAILURE RATES.

Another problem which threatens the validity of the R calculated by this method is the uncertainty of the failure rates of the components of the system. The failure rates used in design are derived from a variety of sources and are almost surely not exactly accurate for any operational system. A realistic way to use design failure rates is to assign confidence limits to their values. With these one can say with a certain confidence that the failure rates of his parts are within a region determined by his confidence limits. This data is often available with design failure rates. Using the two extremes of failure rates, upper and lower confidence limits can be calculated for the mission reliability. The statement can then be made with a certain confidence that the mission reliability is within the interval of its confidence limits. It is instructive to point out that if the failure rates of all parts are perfectly known, there is 100% confidence in the calculated value of mission reliability. If, however, the failure rates are uncertain, as is always the case, confidence limits should be indicated for the mission reliability which reflect the uncertainty of the failure rates.

Estimation of the mission reliability of the system using the failure rates used in design has one serious failing. These failure rates often do not accurately describe the actual components. The design failure rates may have been determined under different environmental conditions than those of system in use, or components in the system may have been subjected to different manufacturing conditions than those used to derive the design failure rates. These and other factors might cause the circuits in the system to have different failure rates than those predicted in original design. Tests performed at t_1 can be used to determine if the actual failure rates are indeed different from design failure rates. If they are different the tests will be used to estimate the actual failure rate.

The first task is to test the null hypothesis that the actual average failure rates are the same as those used in design. To do this, the system must be split into groups of circuits with each group comprised of circuits of identical design. Using the design failure rates, the number of failures that can be expected in each group at t_1 is calculated.

This expected number is $p_j n$, where $p = e^{-\lambda^*_j t}$, and n is the number of circuits in the group. About this expected value one can construct an interval specifying the number of failures he is willing to observe at t_1 and still accept the hypothesis that the actual failure rate is that used in design.

The next step in the procedure is to test the circuits. If possible, all circuits are tested ** and the numbers of failures recorded. If the number of failures at t_1 is n samples is within this interval the design failure rate is used to calculate the mission reliability. If the number of failures is not within the interval a new failure rate is calculated using the observed data at t_1. The mean of this new failure rate is λ_o and is determined from the equation

$$\lambda_o = - \frac{\ln x/n}{t_1}$$

Confidence limits are placed on this calculated rate and the extremes of the confidence interval are used to calculate confidence limits on the estimates of the mission reliability of the system.

The question immediately arises, "Why test the null hypothesis at all if test data is to be accepted in preference to the design failure rates?" This is done because under the condition that the null hypothesis is met, the correspondence of the two sources of failure rate estimates would result in a higher confidence in the final estimate than either source alone can provide. When the null is rejected and the test data alone is used, the confidence in the estimate is reduced.

C. IMPROVEMENT OF THE ESTIMATE THROUGH FAILURE STATE TESTS

In this reliability estimation procedure a more accurate estimate is obtained by testing at t_1 to determine the failure state of the system. If the failure state were known exactly and the failure rates of the circuits were accurate, the mission reliability of the system could be calculated with no equivocation. Thorough testing at t_1 could determine exactly the failure state of the system, but since thorough testing is not of interest in this study the failure state will be known imperfectly. One will have a number of alternatives each with a certain probability given the results of the tests.

---

* λ_j = design failure rate of the $j^{\underline{th}}$ type circuit.

** Note, if the system is too large to permit complete testing, a random sample of each type of circuit is taken and the number of failures observed in the sample is used to estimate the actual failure rates.

Consider again the example of figure Q-1. Each stage of the system has four failure states, zero, one, two, or three failed circuits. If no information is available at t_1, not even that the system is operating, every stage may be in any one of these states. Thus there are 4^2 possible failure states of the system. They have been listed in column 1 of Table 1. Associated with the ith failure state is a probability P_i which is the probability that the system is in this state at t_1 given that all circuits were successful at t_0. Thus, with no information at t_1 on the condition of the system, the probability that the system is in the state in which no circuits have failed is

$$P_1 = p^6$$

The factor p is the probability of success of a circuit at t_1. The probability of the failure state in which one circuit is failed in Stage B is

$$P_2 = 3_p{}^5 (1-p).$$

The probabilities of occurrence of the states given no information on the condition of the system at t_1 are listed in column 5 of Table Q-1.

Associated with each of the failure states is a reliability of the system at t_2 given that the system is in the failure state at t_1. This is written as $R_1(t_2)$ and is shown for each state in column 4 of Table 1.

The reliability of the system is written as the sum over all i of the product of the probability of a ith failure state and the mission reliability given that the system is in the ith state at t_1. Thus:

$$R(t_2) = \sum^{\text{all i}} P_i \; R_i$$

If tests are made at t_1 that give some information on the condition of the system, the number of failure states possible are markedly reduced, and the reliability estimate available at t_1 is much more accurate. For instance if one tests the system of figure Q-1 and finds it functioning correctly at t_1, each stage must have no more than one circuit failure. Thus, only four states are possible after this test. These are states 1, 2, 5 and 6. The probability that the system is in a particular state must be adjusted to account for the known condition that the system functions at t_1. Thus, for the example the probability of being in state 1 with no failures is:

$$\frac{P_1}{\sum_{i = 1,2,5,6} P_i} \qquad (6)$$

The denominator in equation (6) is the probability that the system is in one of the four possible states.

In general, a test to establish the failure state will leave only a set of possible failure states. Assume the test determines the state of the system to such an extent that the only possible failure states are included in the set I. If P_i' is the probability of being in the ith failure state given the results of the tests, then:

$$P_i' = 0 \qquad \text{For } i \notin I$$

Or if a state is not in the set I its probability is zero.

If a state is possible then:

$$P_i' = \frac{P_i}{\sum_{\text{all } i \in I} P_i} \qquad \text{For } i \in I \tag{7}$$

The mission reliability for a particular failure state, R_i, does not change, hence the mission reliability given the results of the test can be written in general as:

$$R_M = \sum^{\text{all } i \in I} \left[\frac{P_i}{\sum_{\text{all } i \in I} P_i} \right] R_i \tag{8}$$

For the example

$$R_M = \frac{1}{P_1 + P_2 + P_5 + P_6} \left[P_1 R_1 + P_2 R_2 + P_5 R_5 + P_6 R_6 \right] \tag{9}$$

More extensive tests at t_1 will further reduce the number of failure states which can exist. For instance if a test reveals that at least one circuit in the network is failed, the failure state which has no errors is eliminated, changing considerably the expected mission reliability. For this example $P_1' = 0$, and states 2, 5 and 6 are the only members of the set I.

To illustrate the value of testing to determine the failure state at t_1, consider the example. The probability that a circuit operates until t_1 is $p(t_1) = 0.9$ and the probability it lasts until t_2, given it was successful at t_1 is $p_m(t_2) = 0.9$. The system is that shown in figure Q-1 and the restoring circuits are assumed perfectly reliable. Say that in reality one circuit is failed in one stage and the circuits in the other stage are all successful, but

this information is unknown to the tester. This is the information to be gained at t_1 through the tests. Table 2 lists the reliability one would predict with different amounts of information about the condition of the system at t_1. The wide variation in the result indicates the importance of testing at t_1.

This section does not propose the detailed procedures for testing a system at t_1. It should, however, indicate the importance of making these tests and the calculations required to utilize the information gained from the test to estimate the system reliability.

TABLE 2

	Test Results at the Mission's Start (t_1)	Predicted System Mission Reliability	Corresponding Risk of Failure
1.	No information at t_1, not even that the system is working.	0.821	0.179
2.	Tests show that the system is working at t_1.	0.867	0.133
3.	Tests show that the system is working but that at least one circuit is failed.	0.770	0.230
4.	Tests show that exactly one circuit in the system is failed at t_1.	0.788	0.212

D. DETERMINING THE MISSION RELIABILITY OF LARGE SYSTEMS

The example of the last section is a small two stage system. One might well ask if it is feasible to enumerate all of the possible failure states of a large system for the determination of the mission reliability. Indeed with no information at t_1 on whether or not an n stage system is operating correctly, there are 4^n possible failure states of the system. As n increases, the number of possible failure states increases exponentially.

The purpose of the tests at t_1 is to eliminate large numbers of these states in the manner shown for the example and hence obtain a better estimate of the mission reliability. The use of equation (8) provides this estimate but it requires, in its present form, separate consideration of each failure state. This is impractical for all but the smallest systems.

This problem is circumvented by first putting the mission reliability equation in a more general form. The mission reliability of the system given the results of the test at t_1 is a conditional probability which can be written:

$$R_M = \frac{\text{Prob. (Test results at } t_1 \text{ and successful system operation at } t_2)}{\text{Prob. (Test results at } t_1)} \qquad (10)$$

Equation 8 is a representation of this equation for small systems.

The form equation (10) takes depends on the characteristics of the system under study and the type of test to which it is subject at t_1. For example, consider an n stage order-three-multiple-line system which has perfect voters. For simplicity assume all the stages are identical with equally reliable circuits. For illustrative purposes assume the stages are arranged in a chain as in figure Q-3.

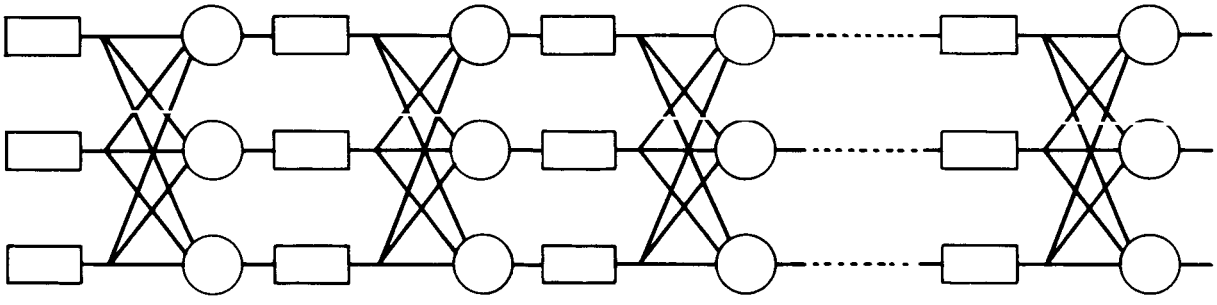

Figure Q-3. Chain of n-Multiple-Line Stages

The first type of test to which the system of figure Q-3 is subjected is a simple test to determine its operability. Is the system failed or successful at t_1? Given the system is successful at t_1 the mission reliability will now be determined.

Because the system is working at t_1, each stage must be in one of two states, either three circuits successful or two circuits successful and one failed. Then the system may be in any one of 2^n possible states. Using equation (8) to evaluate the mission reliability would be a rather tedious and time consuming process if n were a sufficiently large value since both the numerator and denominator of this equation have 2^n terms. However, because of the independence of the stages of the multiple line system, it isn't necessary to carry out this operation. The probability that each stage is successful at t_1 is independent of the condition of all other stages and can be written:

$$\left[p^3 + 3 p^2 (1 - p) \right] \qquad (11)$$

Since they are all identical the probability that all the stages are successful at t_1 is:

$$\left[p^3 + 3p^2(1-p)\right]^n \tag{12}$$

This term is the probability that the system is in a successful failure state at t_1 and is the denominator for equation (10) when the test consists only of determining the operability of the system.

The probability that a single stage is operating at t_2 can be written:

$$\left\{p^3\left[p_m^3 + 3p_m^2(1-p_m)\right] + 3p^2(1-p)\left[p_m^2\right]\right\} \tag{13}$$

Since the stages are independent the probability that system is operating at t_2 is:

$$\left\{p^3\left[p_m^3 + 3p_m^2(1-p_m)\right] + 3p^2(1-p)\left[p_m^2\right]\right\}^n \tag{14}$$

This term is equivalent to the numerator of equation (10). Using the terms (12) and (14) the mission reliability can be determined for this system. Given that the system is successful at t_1 the probability that the system is successful at t_2 is:

$$R_M = \frac{\left\{p^3\left[p_m^3 + 3p_m^2(1-p_m)\right] + 3p^2(1-p)\left[p_m^2\right]\right\}^n}{\left[p^3 + 3p^2(1-p)\right]^n} \tag{15}$$

Note that for this determination of the mission reliability the separate failure states have not been enumerated. The calculation of mission reliability for this system has been a relatively simple procedure.

Other tests at t_1 will result in different forms for the mission reliability equation (10). For instance assume the system of figure 3 is subjected to a different test. This test subdivides the system into three nonredundant ranks as shown in figure Q-4.

Each rank will be tested individually. If a rank fails it can be inferred that one or more circuits in the rank are failed. If a rank is successful it can be inferred that all circuits in the rank are successful.

At t_1 the information is given that the system is operating correctly and that 0, 1, 2 or 3 of the ranks have failed. Now equations must be developed that determine the mission reliability of the system given the results of the test at t_1.

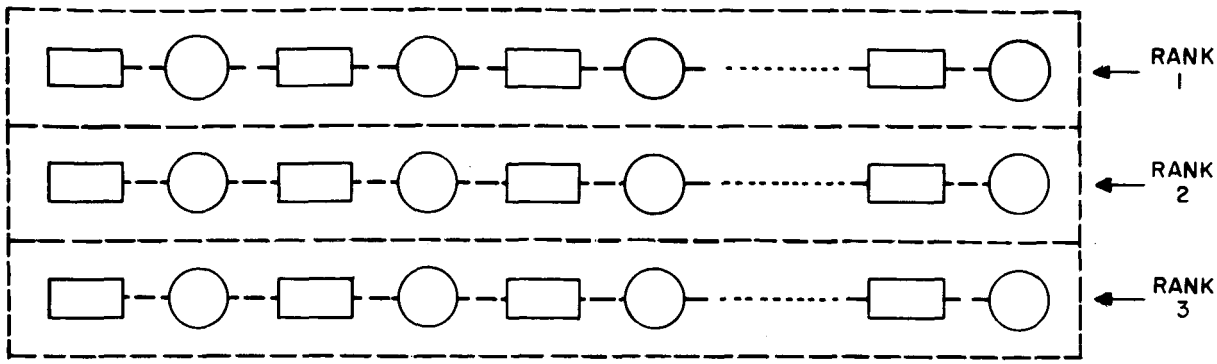

Figure Q-4. System Divided Into Three Nonredundant Ranks

The numerators and denominators of the mission reliability equation for the various test results are shown in Table 3.

TABLE 3

Test Result (Ranks Failed)	Prob. (Test Result at t_1)	Prob. (Test Result at t_1 and Successful System Operation at t_2	Mission Reliability
0	$Y_0 = \left[p^3\right]^n$	$Q_0 = \left[p^3 (p_m^3 + 3p_m^2 (1-p_m))\right]^n$	$\frac{Q_0}{Y_0}$
1	$Y_1 = \left[p^2(1-p) + p^3\right]^n - Y_0$	$Q_1 = \left[p^2(1-p)p_m^2 + p^3(p_m^2 + 3p_m^2(1-p_m)\right]^n - Q_0$	$\frac{Q_1}{Y_1}$
2	$Y_2 = \left[2p^2(1-p) + p^3\right]^n - Y_0 - 2Y_1$	$Q_2 = \left[2p^2(1-p)p_m^2 + p^3(p_m^3 + 3p_m^2(1-p_m)\right]^n - Q_0 - 2Q_1$	$\frac{Q_2}{Y_2}$
3	$Y_3 = \left[3p^2(1-p) + p^3\right]^n - Y_0 - 3Y_1 - 3Y_2$	$Q_3 = \left[3p^2(1-p)p_m^2 + p^3(p_m^3 + 3p_m^2(1-p_m)\right]^n - Q_1 - 3Q_1 - 3Q_2$	$\frac{Q_3}{Y_3}$

Compared to enumerating all the failed states possible with the particular results of a test, these equations are relatively simple. If the assumption that all circuits are equally reliable is removed, the equations for mission reliability are very similar to these except instead of raising a single term to the power n as in these equations, a product of n factors will be taken. This should be a simple matter on a computer.

If the restriction that the restoring circuits be perfectly reliable is removed, the mission reliability equation will not be changed significantly unless the stages are interconnected in such a manner that they are no longer independent. The techniques used to calculate system reliability in this section are invalid if the stages are not independent. Techniques have been developed to determine the reliability of such systems* and these must be used in determining the mission reliability.

The equation describing the mission reliability for a system will depend on both the tests performed at t_1 and the characteristics of the system. These factors will surely be known prior to the test, so equations can be developed to evaluate the mission reliability which take into account the possible failure states of the system without exhaustive enumeration.

E. USING TESTS TO DETERMINE BOTH THE FAILURE STATE OF THE SYSTEM AND FAILURE RATES OF THE CIRCUITS AT t_1

In technique C, tests were made at t_1 to determine the possible failure states of the system. In technique B tests were made to establish the actual failure rate of the circuits of the system. It should be possible to design tests which give information regarding both these parameters.

The tests will establish the failure rate of the system at t_1 and use these in carrying out the reliability calculations described for Technique C. It takes little imagination to see that in the course of tests to determine the failure rate a great deal will be learned about the failure state of the system. For instance as soon as one failure is found the possibility that the system is in the no circuit failure state is decreased to zero, probably decreasing the mission reliability appreciably.

The details of this technique have not been developed, but generally it proposes to use the tests of t_1 to indicate both these parameters and thereby increase markedly the accuracy of the mission reliability estimate.

---

* Jensen, P. A., W. C. Mann and M. R. Cosgrove, "The Synthesis of Redundant Multiple-Line Networks", First Annual Report Contract NONR 3842 (00), May 1, 1963.

IV. TEST OF THE HYPOTHESIS THAT THE MISSION RELIABILITY IS GREATER THAN A REQUIRED VALUE

This method is separated from the others because it does not explicity estimate the reliability of a system. Instead it finds, through measurements at the beginning of the mission, the probability that the system will not meet a given mission reliability specification.

The user of the system must specify the minimum mission reliability. He must also specify the maximum chance he is willing to take that the system does not meet this goal when his tests indicate that it will. It is assumed that the system is not acceptable if the probability that it does not meet the reliability specification is above the given value, and is acceptable otherwise.

The first step in this procedure is to determine the failure rates that the circuits of the system must have to just meet the mission reliability goal. These failure rates are called the maximum failure rates, λ_m. For a system in which many circuits have the same failure rate this does not seem to be too imposing a problem. For example consider a system where all circuits have the same failure rate. If the starting time and duration of the mission are known, the mission reliability can be expressed only as a function of the failure rate, λ. Equation (5) can then be set equal to the required mission reliability and solved for the failure rate. A cut and try method may be required for the solution.

The maximum failure rate is a function of both the starting time, t_1, and the duration, $t_2 - t_1$, of the mission. However, if the duration of the mission is known, it is possible to plot a curve of mission starting time against the maximum failure rate.

Once the maximum failure rate is known it only remains to determine if the actual failure rate of the circuits of the system is less than or equal to this value. This will be determined by testing n of the circuits at t_1 and counting the number of failed circuits. Call the number of failed circuits X_1. With this data and by using the maximum failure rate, an upper bound on the probability that the true failure rate is greater than the maximum failure rate can be determined.

If the fact that a majority of the circuits in a stage must be operative at t_1 is neglected, the success of a circuit in the system may be considered a Bernoulli trial with probability of success, $e^{-\lambda t}$. The probability distribution of the total number of circuit failures in M circuits is then binomial. This distribution or the associated density function can be plotted for any number of samples. One such plot appears in figure Q-5.

The probability distribution of the number of failures at time t_1 can be plotted using the calculated maximum failure rate.

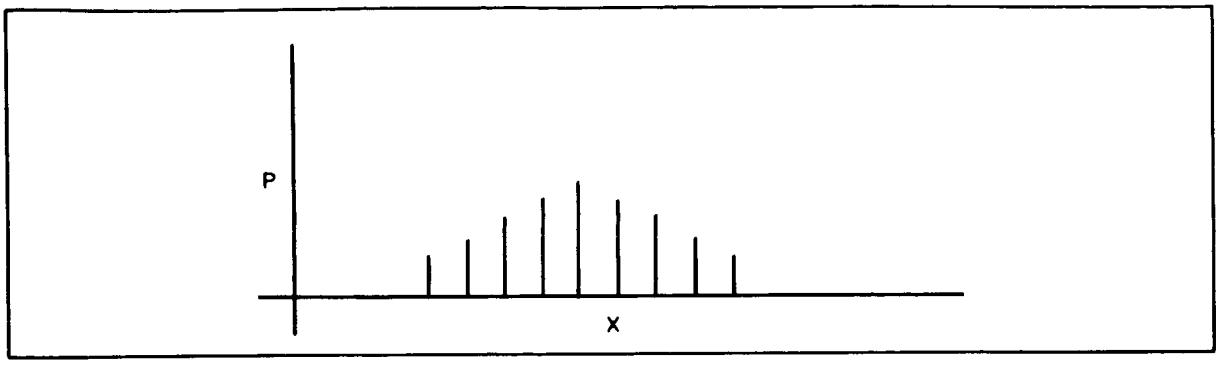

Figure Q-5. Sample Distribution

Some maximum number of failures Y will be chosen such that there is probability of δ that the number of failed circuits observed at t_1, X_1, will be less than Y if the failure rate of the circuits is λ_m. The quantity δ is determined from the binominal:

$$\delta = \sum_{h=0}^{Y-1} \binom{n}{h} \left(e^{-\lambda_m t_1}\right)^{n-h} \left(1 - e^{-\lambda_m t_1}\right)^{h} \qquad (16)$$

For failure rates greater than λ_m the probability that less than Y failures occur must be less than δ. So if X_1 is less than Y, with confidence $1 - \delta$ the statement can be made that the actual failure rate must be less than the maximum failure rate. Now the statement can be made that with confidence $1 - \delta$ that the reliability of the system is greater than the minimum reliability specified by the user.

This method leads to the statement with a confidence $(1 - \delta)$, it can be said that the probability that the system will suceed is R. The information used to compute R might be used to compute the expected time to system failure instead. The object of the test would then be to confirm or reject the hypothesis that the expected life would exceed the mission time with a confidence $(1 - \delta)$. This modification has not been carefully examined but it appears to reduce the number of probabilistic statements from two to one.

This procedure again uses no information on the failure state of the system except that the system is successful at the beginning of the mission. The effect of this on the accuracy of the results has already been discussed in Section IIIC.

V. CONCLUSIONS AND RECOMMENDATIONS

It is the nature of a redundant system to withstand a number of internal failures and still perform its function successfully. This is an extremely desirable property for increasing life or providing high reliability, but it makes it unreasonable to base the decision – whether or not to carry out a mission with the system – only on the fact that the system is operating at the beginning of the mission.

This decision should be based on the probability that the system will complete the mission successfully. There are two major factors affecting the probability which are imperfectly known at the beginning of the mission. First, the number and location of initial circuit failures has a very significant effect on the probability that the system will operate throughout the mission. Second, the mission reliability depends heavily on the failure rates of the circuits which make up the system. There is little accurate information concerning either of these factors when it is time to make the decision.

The report proposes that certain tests be made just before the mission is to begin to determine at least approximately, these unknowns. It proposes some procedures for using the results of the tests to estimate the mission reliability with varying degrees of accuracy. A procedure for making the decision on the useability of the system without estimating the mission reliability is also presented.

It should be noted that the details of these procedures are still to be worked out and the accuracy of their results are still uncertain. The work here reported will provide the basis for future studies on the subject.

No attempt has been made to evaluate the relative usefulness of these procedures. It is recommended that efforts be made to develop an appropriate measure for comparing the techniques so that they may be evaluated relative to a common scale.

One very important area of study neglected by this report is the design of simple and efficient tests to be performed at the beginning of the mission to obtain the information required for the reliability estimates. As much information as possible must be gained from a minimum number of tests. A small amount of basic work has been done in this area, and it will be the subject of future efforts.

BIBLIOGRAPHY

1) J. von Neuman, "Probabilistic Logics and the Synthesis of Reliable Organisms from Unreliable Components in Automata Studies, "Ed. C. E. Shannon and J. McCarthy, Princeton University Press, 1956.

2) W. H. Pierce, "Adaptive Vote-Takers Improve the Use of Redundancy, " Redundancy Techniques for Computing Systems. " Ed. R. H. Wilcox and W. C. Mann, Spartan Books, 1962. July 17, 1961

3) "A Survey of Adaptive Components for Use in Failure Free Systems", Special Technical Report No. 1, Nasw-572, Aug. 1963.

4) W. C. Mann, "Restorative Processes for Redundant Computing Systems, " Redundancy Techniques for Computing Systems, Ed R. H. Wilcox and W. C. Mann, Spartan Books, 1962.

5) A. R. Helland, W. C. Mann, "Failure Effects in Redundant Systems, " Report No. EE-3351, Westinghouse Electronics Division 1963.